



# POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

VERSIÓN 3

UNIDAD DE BUSQUEDA DE PERSONAS DADAS POR DESAPARECIDAS



## Tabla de contenido

<b>I.</b>	<b>PRESENTACIÓN</b>	<b>2</b>
<b>II.</b>	<b>OBJETIVOS</b>	<b>3</b>
	<b>2.1 Objetivo General</b>	<b>3</b>
	<b>2.2 Objetivos Específicos</b>	<b>3</b>
<b>III.</b>	<b>ALCANCE</b>	<b>3</b>
<b>IV.</b>	<b>METODOLOGÍA APLICADA</b>	<b>3</b>
<b>V.</b>	<b>VIGENCIA</b>	<b>4</b>
<b>VI.</b>	<b>PERIODICIDAD</b>	<b>4</b>
<b>VII.</b>	<b>CONTEXTO ESTRATÉGICO</b>	<b>4</b>
<b>VIII.</b>	<b>CONCEPTOS CLAVE</b>	<b>4</b>
<b>IX.</b>	<b>NORMATIVIDAD</b>	<b>9</b>
<b>X.</b>	<b>DEFINICIÓN DE ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO</b>	<b>11</b>
<b>XI.</b>	<b>LÍNEAMIENTOS PARA LA ADMINISTRACIÓN DEL RIESGO</b>	<b>13</b>
	<b>11.1 Identificación de riesgos</b>	<b>13</b>
	11.1.1. Riesgos de gestión	13
	11.1.2 Riesgos de corrupción	14
	11.1.3 Riesgos fiscales	14
	11.1.4 Riesgos de seguridad de la información	15
	<b>11.2. Valoración de riesgos</b>	<b>15</b>
	11.2.1 Análisis de riesgos	15
	a. Criterios para el análisis de riesgos de gestión y de seguridad de la información	15
	• Definición del nivel de probabilidad	16
	• Calificación del impacto	16
	b. Criterios para el análisis de riesgos de corrupción	17
	• Definición del nivel de probabilidad	17
	• Calificación del impacto	17
	c. Criterios para el análisis de riesgos fiscales	18
	• Definición del nivel de probabilidad	18
	• Calificación del impacto	18
	11.2.2 Evaluación de riesgos	19
	a. Determinación del nivel de severidad	19
	b. Valoración de controles	20
<b>XII.</b>	<b>ESTRATEGIAS PARA COMBATIR EL RIESGO</b>	<b>22</b>
<b>XIII.</b>	<b>MONITOREO Y REVISIÓN DEL RIESGO</b>	<b>24</b>
<b>XIV.</b>	<b>TRATAMIENTO DE RIESGOS MATERIALIZADOS</b>	<b>25</b>
<b>XV.</b>	<b>EVALUACIÓN</b>	<b>26</b>
<b>XVI.</b>	<b>MONITOREO Y REVISIÓN</b>	<b>26</b>
<b>XVII.</b>	<b>SEGUIMIENTO Y EVALUACIÓN INDEPENDIENTE</b>	<b>27</b>
<b>XVIII.</b>	<b>DIVULGACIÓN</b>	<b>27</b>

## I. PRESENTACIÓN

La Unidad de Búsqueda de Personas dadas por Desaparecidas en el contexto y en razón del conflicto armado (en adelante UBPD) se encuentra comprometida con el fortalecimiento de la cultura de la prevención. Por lo tanto, dentro de su Sistema de Gestión, se identifican y gestionan los riesgos institucionales que puedan afectar, el cumplimiento del mandato legal, la integralidad en el cumplimiento de la misión, el carácter humanitario y extrajudicial, los principios rectores para la búsqueda de personas desaparecidas, el manejo eficiente y transparente de los recursos, la construcción de relaciones de confianza, y la satisfacción de los derechos a la verdad y a la reparación de las víctimas, como aporte a la construcción de paz en el marco del Sistema Integral de Verdad, Justicia, Reparación y No Repetición.

Teniendo en cuenta que la gestión del riesgo es un factor estratégico para la UBPD al permitir que se identifiquen y evalúen los posibles eventos o situaciones que pueden afectar negativamente a la entidad y definir acciones preventivas a fin de mitigar su materialización e impacto sobre el desempeño y cumplimiento de los objetivos a corto, mediano y largo plazo de la entidad, además de proporcionar información valiosa para tomar decisiones estratégicas; desde el liderazgo de la Alta Dirección y con la participación del Comité Institucional de Coordinación de Control Interno - CICCI se formula esta política de Administración del Riesgo Institucional.

Por otro lado, es pertinente señalar que teniendo en cuenta la naturaleza jurídica de la UBPD y según lo definido en el concepto técnico emitido por el Departamento Administrativo de Función Pública<sup>1</sup> del 02 de febrero de 2019, la política atiende lo dispuesto en la Dimensión 7 del Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG y a lo expresado en el Modelo Estándar de Control Interno (MECI) en relación con el tema de riesgos.

A través de la Política de Administración del Riesgo se adoptan los lineamientos para la adecuada administración (tratamiento, manejo y seguimiento) del riesgo en sus diferentes tipologías, que permita alcanzar un nivel aceptable de riesgo en los procesos de la entidad.

Tales lineamientos reflejan los requisitos basados en gestión del riesgo, desde un enfoque de preventivo, reduciendo los posibles efectos de su materialización y estableciendo el tratamiento de los mismos, con el propósito de disminuir la vulnerabilidad frente a situaciones que puedan interferir en el cumplimiento de su mandato.

---

<sup>1</sup> Concepto Técnico del 02 de febrero de 2019 emitido por el Departamento Administrativo de Función Pública del 02 de febrero de 2019 en el cual expresa claramente que "La reglamentación a aplicar frente al Sistema de Control Interno, son las disposiciones establecidas en la Ley 87 de 1993, y sus Decretos reglamentarios, específicamente el artículo 2.2.23.2 del Decreto 1499 de 2017, mediante el que se actualiza la estructura del Modelo Estándar de Control Interno MECI. "Respecto a los lineamientos o criterios para la actualización del Modelo Estándar de Control Interno, su entidad debe consultar la Dimensión 7 del Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG, en donde se detalla la nueva estructura. En este sentido, dicha actualización deberá responder a la estructura de cinco componentes a saber: (i) Ambiente de control, (ii) Evaluación del riesgo, (iii) Actividades de control, (iv) Información y comunicación y (v) Actividades de monitoreo, así como con la articulación con el modelo de las tres líneas de defensa", la UBPD, tomará en cuenta únicamente, lo expresado por el modelo para el Modelo Estándar de Control Interno (MECI) y lo que allí se relacione en temas de riesgos.

## **II. OBJETIVOS**

### **2.1 Objetivo General**

Definir orientaciones y/o lineamientos para la adecuada administración (tratamiento, manejo y seguimiento) del riesgo que permitan alcanzar un nivel aceptable de los mismos en los procesos de la entidad mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales, contribuyendo al cumplimiento de sus funciones y en el logro de los objetivos estratégicos de la UBPD.

### **2.2 Objetivos Específicos**

- Disminuir la vulnerabilidad frente a situaciones que puedan interferir en el cumplimiento de las funciones y en el logro de los objetivos de la Entidad.
- Generar instrumentos y/o mecanismos para monitorear y evaluar la implementación de las acciones para la administración del riesgo en la UBPD
- Generar cultura de autocontrol y autoevaluación en todos los servidores de la entidad frente a la gestión del riesgo.
- Contribuir a la protección de los recursos de la UBPD frente a la ineficiencia en la gestión y las amenazas de corrupción.

## **III. ALCANCE**

La Política de Administración de Riesgos de la UBPD, aplica para todos los niveles, áreas y procesos de la Entidad e involucra la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y el análisis de los riesgos: de gestión, de seguridad de la información, los riesgos fiscales y los correspondientes a corrupción, asociados a cada uno de los procesos definidos por la entidad.

Esta política no incluye el Sistema de Administración de Riesgos de Lavados de Activos y Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva SARLAFT / FPADM, el cual se incluirá en la formulación e implementación del Programa de Transparencia y Ética Pública PTEP de la Unidad de Búsqueda de Personas dadas por desaparecidas.

## **IV. METODOLOGÍA APLICADA**

La Política de administración de riesgos de la UBPD, esta alineada con las directrices emitidas por el Departamento Administrativo de la Función Pública – DAFP a través de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas (Versión 6), en las etapas de contexto estratégico, identificación, análisis, evaluación, monitoreo y revisión, y seguimiento; y se estructura bajo un enfoque preventivo de evaluación de la gestión y el control de los riesgos, en el marco de la mejora continua.

El diseño, implementación y seguimiento de los riesgos de prevención de daño antijurídico seguirán los lineamientos u orientaciones dadas por la Agencia Nacional de Defensa Jurídica del Estado, y los riesgos en los procesos de contratación seguirán los lineamientos u orientaciones dadas de la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente. Estos se regirán igualmente por las demás metodologías y

políticas públicas que se impartan sobre la materia y que apliquen a la UBPD dada su naturaleza humanitaria y extrajudicial.

## **V. VIGENCIA**

La presente Política rige a partir de su aprobación por parte del Comité Institucional de Coordinación de Control Interno y permanece vigente hasta una nueva actualización.

## **VI. PERIODICIDAD**

La revisión y/o actualización de los mapas de riesgos de Gestión, Corrupción y Seguridad de la Información - Seguridad Digital se realizará como mínimo 1 vez al año o cuando las circunstancias lo ameriten, a partir de modificaciones o cambios sustanciales en el contexto estratégico, cambios relevantes en los procesos y/o procedimientos, o cualquier otra circunstancia que afecte el funcionamiento de la entidad.

La periodicidad del monitoreo para los riesgos de Gestión y Seguridad de la Información – Seguridad Digital se realizará ,mínimo 1 vez al año, mientras que para los riesgos de Corrupción este monitoreo se realizará mínimo 3 veces al año de manera cuatrimestral.

## **VII. CONTEXTO ESTRATÉGICO**

Como insumo para la identificación de los riesgos en el anexo 1 se presentan las matrices DOFA que resumen la revisión del contexto estratégico de la entidad tanto interno como externo. A partir de este cada líder de proceso deberá identificar como este contexto se refleja en dicho proceso e identificar los riesgos asociados particularmente teniendo en cuenta las debilidades y amenazas identificadas.

## **VIII. CONCEPTOS CLAVE**

De conformidad con la Guía para la Administración del Riesgo<sup>2</sup> expedida por el Departamento Administrativo de la Función Pública, las normas técnicas para la gestión de riesgos, la normatividad aplicable y los procedimientos de la entidad, la política de Administración de Riesgos se fundamenta en los siguientes conceptos:

- Activo<sup>3</sup>: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

---

<sup>2</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, 2022.

<sup>3</sup> Norma ISO 27000:2018

- **Apetito del riesgo<sup>4</sup>:** es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano del Gobierno. El apetito del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Bien público<sup>5</sup>:** Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así: a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc. b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.
- **Capacidad del riesgo<sup>6</sup>:** es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la entidad.
- **Causa<sup>7</sup>:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa Eficiente o Causa Adecuada<sup>8</sup>:** Es el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño.
- **Causa Inmediata<sup>9</sup>:** circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Nota: Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (Causa Inmediata, pero se asocia a la misma causa inmediata).

- **Causa Raíz<sup>10</sup>:** causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo.
- **Confidencialidad<sup>11</sup>:** propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

---

<sup>4</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, 2022.

<sup>5</sup> Ibid.

<sup>6</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, 2022

<sup>7</sup> Ibid.

<sup>8</sup> Ibid.

<sup>9</sup> Ibid.

<sup>10</sup> Ibid.

<sup>11</sup> Ibid.

- Consecuencia<sup>12</sup>: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Nota: Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos.

- Control<sup>13</sup>: medida que permite reducir o mitigar el riesgo.
- Disponibilidad<sup>14</sup>: propiedad de ser accesible y utilizable a demanda por una entidad.
- Factores de riesgo<sup>15</sup>: Son las fuentes generadoras de riesgo.
- Gestión del Riesgo Fiscal<sup>16</sup>: son las actividades que debe desarrollar cada Entidad y todos los gestores públicos para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).
- Gestor público<sup>17</sup>: Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales. A título de ejemplo, además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.
- Gestor Fiscal<sup>18</sup>: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique). A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.
- Impacto<sup>19</sup>: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

---

<sup>12</sup> Ibid.

<sup>13</sup> Ibid.

<sup>14</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, 2022.

<sup>15</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, 2022.

<sup>16</sup> Ibid.

<sup>17</sup> Ibid.

<sup>18</sup> Ibid.

<sup>19</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, 2020.

- Integridad<sup>20</sup>: propiedad de exactitud y completitud.
- Intereses patrimoniales de naturaleza pública<sup>21</sup>: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas. Ejemplos: Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas; la participación accionaria pública en una empresa de economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe; explotación de bienes públicos y/o recaudo de recursos públicos por un particular sin contrato o habilitación legal.
- Nivel de riesgo<sup>22</sup>: es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad \* Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.
- Patrimonio público<sup>23</sup>: se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica.
- Probabilidad<sup>24</sup>: se entiende como la posibilidad de ocurrencia del riesgo; estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.
- Probabilidad Inherente<sup>25</sup>: número de veces que se pasa por el punto de riesgo en el periodo de un (1) año.
- Punto de Riesgo:<sup>26</sup>Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública. Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales.

---

<sup>20</sup>Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, 2022.

<sup>21</sup>Ibid.

<sup>22</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, 2022.

<sup>23</sup> Artículo 6 Ley 610 de 2000 y sentencia C-340-07.

<sup>24</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, 2020.

<sup>25</sup> Ibid.

<sup>26</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, 2022.

- Recurso público<sup>27</sup>: Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.
- Riesgo<sup>28</sup>: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

- Riesgo de Seguridad de la información<sup>29</sup>: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- Riesgo de corrupción<sup>30</sup>: posibilidad de que, por acción u omisión, se use del poder para desviar la gestión de lo público hacia un beneficio privado.
- Riesgo fiscal<sup>31</sup>: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial. (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).
- Riesgo inherente<sup>32</sup>: nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel de riesgo inherente, dentro de unas escalas de severidad.
- Riesgo residual<sup>33</sup>: resultado de aplicar la efectividad de los controles al riesgo inherente.
- Tolerancia del riesgo<sup>34</sup>: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.
- Vulnerabilidad<sup>35</sup>: representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

---

<sup>27</sup> Ibid

<sup>28</sup> Ibid.

<sup>29</sup> Ibid.

<sup>30</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, 2022.

<sup>31</sup> Ibid

<sup>32</sup> Ibid.

<sup>33</sup> Ibid.

<sup>34</sup> Ibid.

<sup>35</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, 2022.

## **IX. NORMATIVIDAD**

La Constitución Política de Colombia, en sus artículos 209 y 269, incorporó el control interno como un instrumento orientado a garantizar el logro de los objetivos de cada entidad del Estado y el cumplimiento de los principios que rigen la función pública.

Ley 87 de 1993, artículo 2°, literales a) y f), los cuales establecen que el control interno está orientado a la protección de los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten, y a definir y aplicar medidas para prevenirlos, así como detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.

Ley 1474 de 2011, Estatuto Anticorrupción, el cual dispone en su artículo 73 que todas las entidades deben elaborar anualmente un Plan Anticorrupción y de Atención al Ciudadano, el cual debe incluir el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti-tramites y los mecanismos para mejorar la atención al ciudadano.

Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del derecho de Acceso a la Información Pública Nacional; en el literal g) del artículo 9 establece el deber de publicar el Plan Anticorrupción y de Atención al Ciudadano, en los sistemas de información del Estado o herramientas que lo sustituyan.

Decreto 1083 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública; señala en su artículo 2.2.21.3.2 que los elementos mínimos del Sistema de Control Interno mencionados en la Ley 87 de 1993 y demás normativa relacionada, conforman cinco (5) grupos que se interrelacionan y que constituyen los procesos fundamentales de la administración: Dirección, Planeación, Organización, Ejecución, Seguimiento y Control (Evaluación). Así mismo, señala que los responsables de fortalecer la interrelación y funcionamiento armónico de los elementos que conforman estos 5 grupos son los servidores públicos en cumplimiento de las funciones asignadas en la normativa vigente, de acuerdo con el área o dependencia de la cual hacen parte.

Decreto 1499 de 2017, que actualiza el Modelo Integrado de Planeación y Gestión - MIPG, articulando “el nuevo Sistema de Gestión, que integra los anteriores sistemas de Gestión de Calidad y de Desarrollo Administrativo, con el Sistema de Control Interno actualizado también en la séptima dimensión”<sup>36</sup>, con el fin de “consolidar, en un solo lugar, todos los elementos que se requieren para que una organización pública funcione de manera eficiente y transparente, y que esto se refleje en la gestión del día a día”<sup>37</sup>.

Es necesario precisar que el Decreto 1499 de 2017 estableció en su artículo 2.2.22.3.4. el Ámbito de aplicación precisando que “El Modelo Integrado de Planeación y Gestión (MIPG) se adoptará por los organismos y entidades de los órdenes nacional y territorial de la rama ejecutiva del poder público. En el caso de las entidades descentralizadas con capital público y privado, el modelo aplicará en aquellas en que el Estado posea el 90% o más del capital social. Las entidades y organismos estatales sujetos a régimen especial, de conformidad con lo señalado en el artículo 40 de la Ley 489 de 1998, las ramas legislativa y judicial, la organización electoral, los organismos de control y los institutos científicos y tecnológicos, aplicarán la política de control interno prevista en la Ley 87 de 1993; así mismo, les aplicarán las demás políticas de gestión y desempeño institucional

<sup>36</sup> Presidencia de la República, Departamento Administrativo de la Función Pública. Modelo Integrado de Planeación y Gestión – MIPG. Pág. 5

<sup>37</sup> *Ibíd.*

en los términos y condiciones en la medida en que les sean aplicables de acuerdo con las normas que las regulan.”

En virtud del Acto Legislativo 01 de 2017, el Gobierno Nacional expidió el Decreto Ley 589 de 2017 “Por el cual se organiza la Unidad de Búsqueda de Personas dadas por Desaparecidas en el contexto y en razón del conflicto armado”, señalando conforme al párrafo primero del artículo primero que: “La UBPD es una entidad del Sector Justicia, de naturaleza especial, con personería jurídica, autonomía administrativa y financiera, patrimonio independiente y un régimen especial en materia de administración de personal”.

No obstante, la incorporación de la Unidad dentro del sector justicia, no implica que esté sujeta a un control jerárquico o de tutela por parte del Ministerio de Justicia y del Derecho, tal como lo sostiene la Corte Constitucional en su Sentencia C-067 de 20 de junio de 2018, así:

“(…) Desde esta perspectiva, y contrario a lo que sostienen los intervinientes, la referencia al sector justicia, no implica que la Unidad esté orgánicamente sujeta al Ministerio de Justicia y del Derecho, ya que no se consagra la existencia de una relación de adscripción o de vinculación para el ejercicio de sus funciones, circunstancia que sólo sería posible al tratarse de un organismo descentralizado, lo cual no corresponde con lo señalado ni en el Acto Legislativo 01 de 2017, ni el Decreto Ley 589 de 2017, en donde se señala que la UBPD es un organismo del orden nacional, con naturaleza jurídica especial”.

Por lo anterior, y teniendo en cuenta la naturaleza jurídica de la UBPD y el concepto técnico emitido por el Departamento Administrativo de Función Pública del 02 de febrero de 2019 en el cual expresa claramente que “La reglamentación a aplicar frente al Sistema de Control Interno, son las disposiciones establecidas en la Ley 87 de 1993, y sus Decretos reglamentarios, específicamente el artículo 2.2.23.2 del Decreto 1499 de 2017, mediante el que se actualiza la estructura del Modelo Estándar de Control Interno MECI. “Respecto a los lineamientos o criterios para la actualización del Modelo Estándar de Control Interno, su entidad debe consultar la Dimensión 7 del Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG, en donde se detalla la nueva estructura. En este sentido, dicha actualización deberá responder a la estructura de cinco componentes a saber: (i) Ambiente de control, (ii) Evaluación del riesgo, (iii) Actividades de control, (iv) Información y comunicación y (v) Actividades de monitoreo, así como con la articulación con el modelo de las tres líneas de defensa”, la UBPD, tomará en cuenta únicamente, lo expresado por el modelo para el Modelo Estándar de Control Interno (MECI) y lo que allí se relacione en temas de riesgos.

Decreto 648 de 2017, el cual modificó el nombre del artículo 2.2.21.3.2 del Decreto 1083 de 2015, de “Elementos de la Unidad Básica del Sistema” por “Elementos del Sistema Institucional de Control Interno”.

Decreto 1393 de 2018, por el cual se establece la estructura interna de la Unidad de Búsqueda de Personas dadas por Desaparecidas en el contexto y en razón del conflicto armado (UBPD) y se determinan las funciones de sus dependencias. Esta norma precisa en el artículo el artículo 4, numeral 9, establece como función de la Oficina Asesora de Planeación “Orientar y coordinar la implementación, mantenimiento y mejora del Sistema Integrado de Gestión”. Y en el 8, numeral 17, que una de las funciones para la Oficina de Control Interno es “Asesorar a las dependencias de la Unidad en la identificación y prevención de los riesgos que puedan afectar el logro de sus objetivos.”

## X. DEFINICIÓN DE ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El Sistema de Control Interno está integrado por el esquema de organización y el conjunto de planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y de los recursos, se lleven a cabo de acuerdo con las normas constitucionales y legales vigentes, dentro de las políticas trazadas por la alta dirección y en atención a las metas u objetivos previstos. Adicionalmente, la estructura del MECI se acompaña por un esquema de asignación de responsabilidades, adaptado del Modelo “*Líneas de Defensa*”, el cual otorga responsabilidad a todos los niveles de la Entidad. A continuación, se relacionan los roles y responsabilidades de cada línea de defensa establecida en el Modelo Estándar de Control Interno<sup>38</sup>.

Para la implementación del Modelo Estándar de Control Interno, los roles y responsabilidades para la administración de riesgos están dados por el modelo de las líneas de defensa, así:

Tabla 1. Roles y responsabilidades según línea de defensa. UBPD, 2024

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	Alta Dirección  Comité Institucional de Coordinación de Control Interno - CICC	El CICC establece y aprueba la Política de Administración del Riesgo la cual incluye los niveles de responsabilidad y autoridad.  El CICC define y hace seguimiento a los niveles de aceptación del riesgo anualmente.  La Alta Dirección analiza los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles.  El CICC realiza seguimiento y análisis anualmente a los riesgos institucionales.  El CICC anualmente evalúa y da línea sobre la administración de los riesgos en la UBPD.  La Alta Dirección anualmente evalúa el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento de este.
Primera Línea	Líderes de procesos, líderes operativos de proyectos de la entidad y equipos territoriales.  Servidores(as) en General	Los servidores(as) en general implementan acciones correctivas, igualmente detectan las deficiencias de control en el día a día.  Los líderes de los procesos identifican y valoran los riesgos que pueden afectar los planes, proyectos y procesos a su cargo y los actualizan cuando se requieran.  Los servidores(as) en general gestionan constantemente los riesgos con base en la política de administración del riesgo e implementan las metodologías y lineamientos para ello.

<sup>38</sup> Departamento Administrativo de la Función Pública. DAFP (2022). “Guía para la administración del riesgo y el diseño de controles en entidades públicas” Versión 6.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		<p>Los líderes de procesos elaboran y/o actualizan los mapas de riesgo, incluidos los riesgos de corrupción. Cada vez que la segunda línea de defensa lo requiera.</p> <p>Los servidores(as) en general definen, aplican y hacen seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras a la gestión del riesgo en su proceso.</p> <p>Los líderes de los procesos proponen mejoras a la gestión del riesgo en su proceso y reportan en el sistema o esquema definido por la entidad los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos</p> <p>Los líderes de proceso monitorean la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, evalúan la eficiencia, eficacia y efectividad de los controles y determinan las acciones de mejora a que haya lugar, así como realizan monitoreo a las acciones de mejora establecidas.</p> <p>Los líderes de proceso informan a la Oficina Asesora de Planeación (segunda línea) sobre los riesgos materializados en los planes, proyectos y/o procesos a su cargo. En caso de la materialización de un riesgo no identificado, este debe ser incluido en el mapa de riesgo del proceso correspondiente.</p> <p>Los líderes de proceso establecen y aplican las acciones de mejora requeridas frente al mapa de riesgos correspondiente, una vez se genera el informe de materialización del riesgo.</p> <p>Los líderes de proceso reportan a la Oficina de Control Interno (tercera línea de defensa) sobre los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.</p>
Segunda Línea	Oficina Asesora de Planeación.	<p>Consolida y socializa el mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y lo presenta para análisis y seguimiento ante el Comité</p> <p>Orienta a los líderes de procesos y a su equipo de trabajo en la identificación y valoración de los riesgos a su cargo, de acuerdo con la metodología y lineamientos establecidos por la Entidad e incorporando los riesgos de corrupción.</p> <p>Monitorea los controles y acciones establecidos por la primera línea de defensa de acuerdo con la información suministrada por los líderes de procesos.</p>
Segunda Línea	Oficina de Tecnología de Información y Comunicaciones, Líder de Seguridad de la Información.	<p>Orienta a los líderes de proceso en la identificación y valoración de los riesgos de seguridad de la información, de acuerdo con los lineamientos establecidos en la Entidad para este fin.</p> <p>Monitorea los controles y acciones de los riesgos de seguridad de la información establecidos por la primera línea de defensa de acuerdo con la información suministrada por los líderes de procesos.</p>
Tercera Línea	A cargo de la Oficina de Control Interno	<p>Evalúa de forma independiente y objetiva la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción.</p>

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		<p>Da a conocer a toda la entidad el Plan Anual de Auditorías basado en riesgos y los resultados de la evaluación de la gestión del riesgo.</p> <p>Identifica y evalúa cambios que podrían tener un impacto significativo en el Sistema de Control Interno durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna, e informa al Comité Institucional de Coordinación de Control Interno. - CICCI</p> <p>Revisa la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos de la entidad.</p> <p>Alerta sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.</p> <p>Alerta sobre la identificación y materialización de riesgos de corrupción, gestión y seguridad de la información</p> <p>Recomienda mejoras a la política de administración del riesgo.</p>

## XI. LÍNEAMIENTOS PARA LA ADMINISTRACIÓN DEL RIESGO

### 11.1 Identificación de riesgos

La identificación de riesgos permite determinar los riesgos que se encuentran o no bajo el control de la UBPD. En la identificación de los riesgos se deberá tener en cuenta:

- Contexto estratégico
- Caracterización de los procesos
- Análisis de factores internos y externos que pueden derivar en riesgos que afecten el cumplimiento de los objetivos

#### 11.1.1. Riesgos de gestión

Para la identificación de los riesgos de gestión se debe empezar por el análisis de los objetivos, tanto estratégicos como de cada uno de los procesos, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento de estos, posteriormente se deben aplicar las siguientes fases:

- **Identificación de los puntos de riesgo:** son estas actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control.
- **Identificación del área de impacto:** es la consecuencia económica o reputacional a la cual se ve expuesta la Entidad en caso de la materialización de un riesgo.
- **Identificación de áreas de factores de riesgo:** son las fuentes generadoras del riesgo.

- **Descripción del Riesgo:** debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso.
- **Clasificación del Riesgo:** permite agrupar los riesgos identificados.

### 11.1.2 Riesgos de corrupción

Los riesgos de corrupción se establecen sobre procesos. Con el fin de facilitar su identificación y evitar confusiones con los riesgos de gestión, se utiliza la siguiente matriz cuyo chequeo permite determinar si se encuentra ante un riesgo de corrupción.

Tabla 2. Matriz de definición de riesgos de corrupción. UBPD, 2023

Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio Privado
(Ejemplo) Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas – DAFP Versión 6; diciembre 2022.

### 11.1.3 Riesgos fiscales

Para la identificación del riesgo fiscal es necesario establecer:

- **Puntos de riesgo fiscal:** Son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas. En conclusión, los puntos de riesgo fiscal son todas las actividades que representan gestión fiscal, así mismo, se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal.<sup>39</sup>
- **Circunstancias Inmediatas:** situación o actividad bajo la cual se presenta el riesgo, pero no constituye la causa principal o básica; o causa raíz para que se presente el riesgo, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.
- **Identificación de áreas de impacto:** el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

<sup>39</sup> Departamento Administrativo de la Función Pública (2022). Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 6. Pág. 69.

- **Identificación de causa raíz o hecho generador:** La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menos cabo, disminución, perjuicio, detrimento, pérdida o deterioro.
- **Descripción del Riesgo Fiscal:** Se debe iniciar con “posibilidad de” + impacto + circunstancia inmediata + causa raíz.

#### **11.1.4 Riesgos de seguridad de la información**

Los riesgos de seguridad de la información estarán asociados a la pérdida de uno o más de los siguientes factores:

- Pérdida de Confidencialidad
- Pérdida de Integridad
- Pérdida de Disponibilidad

Para la identificación de los riesgos de seguridad de la información, se debe realizar inicialmente la identificación de activos de información, esto permite determinar la importancia de estos para el proceso o la entidad, esta identificación se debe realizar de acuerdo con los procedimientos establecidos por la entidad (Guía de Gestión de Activos de Información). Para cada activo o grupo de activos específicos del proceso con valoración alta se debe realizar la identificación del riesgo asociado, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

### **11.2. Valoración de riesgos**

#### **11.2.1 Análisis de riesgos**

En el análisis del riesgo se deben considerar los aspectos de calificación y evaluación del riesgo; además dependerá de la información obtenida, de la identificación de riesgos y de la disponibilidad de datos históricos y aportes de los servidores de la organización.

El análisis busca establecer la **probabilidad de ocurrencia** de los riesgos y el **impacto** de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el **nivel de riesgo** (riesgo inherente) y las acciones que se van a implementar.

- **Probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo y estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo la probabilidad inherente será el número de veces que pasa por el punto de riesgo en el periodo de un año.
- **Impacto:** Se entiende como las consecuencias que puede ocasionar a la Entidad la materialización del riesgo.

#### **a. Criterios para el análisis de riesgos de gestión y de seguridad de la información**

- **Definición del nivel de probabilidad**

En la siguiente tabla se establecen los criterios para definir el nivel de probabilidad de los riesgos de gestión, y seguridad de la información:

Tabla 3. Criterios para definir la probabilidad de los riesgos de gestión y seguridad de la información. UBPD, 2023

	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
<b>Muy Baja</b>	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
<b>Baja</b>	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
<b>Media</b>	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
<b>Alta</b>	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
<b>Muy Alta</b>	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas – DAFP Versión 6; diciembre 2022.

- **Calificación del impacto**

Para determinar el impacto se debe analizar el tipo de afectación que tendría la Entidad en caso de materialización del riesgo, si esta afectación es económica (dinero, multas, sanciones) o reputacional (imagen de la Entidad), en caso de que en el análisis se concluya que la materialización genera las dos afectaciones (dinero e imagen) se debe elegir la de nivel más alto. En la siguiente tabla se establecen los criterios para definir el nivel de impacto de los riesgos de gestión y de seguridad de la información:

Tabla 4. Criterios para definir el nivel de impacto de los riesgos de gestión y seguridad de la información. UBPD, 2023

	AFECTACIÓN ECONÓMICA	AFECTACIÓN REPUTACIONAL
<b>Leve 20%</b>	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
<b>Menor 40%</b>	Entre 10 y 50 SMLMV.	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
<b>Moderado 60%</b>	Entre 50 y 100 SMLMV.	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
<b>Mayor 80%</b>	Entre 100 y 500 SMLMV.	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.

<b>Catastrófico 100%</b>	Mayor a 500 SMLMV.	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.
--------------------------	--------------------	--

Fuente: Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas – DAFP; Versión 6; diciembre 2022.

**b. Criterios para el análisis de riesgos de corrupción**

• **Definición del nivel de probabilidad**

En la siguiente tabla se establecen los criterios para definir el nivel de probabilidad de los riesgos de corrupción

Tabla 5. Criterios para definir la probabilidad de los riesgos de corrupción. UBPD, 2023

Nivel	Descriptor	Descriptor	Frecuencia
5	<b>Casi seguro</b>	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	<b>Probable</b>	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos una vez en el último año.
3	<b>Posible</b>	El evento podrá ocurrir en algún momento.	Al menos una vez en los últimos 2 años.
2	<b>Improbable</b>	El evento puede ocurrir en algún momento.	Al menos una vez en los últimos 5 años.
1	<b>Rara Vez</b>	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años.

Fuente: Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas – DAFP Versión 6; diciembre 2022.

• **Calificación del impacto**

Para el caso de los riesgos de corrupción, los criterios para calificar el impacto son:

Tabla 6. Criterios para definir el nivel de impacto de los riesgos de corrupción. UBPD, 2023

No.	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		

No.	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SI	NO
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

**Nota:** Por cada riesgo de corrupción identificado, se debe diligenciar la tabla anterior.

Fuente: Departamento Administrativo de la Función Pública- DAFP (2022). Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 6.

Tabla 7. Calificación del impacto de los riesgos de corrupción. UBPD, 2023

MODERADO	Genera medianas consecuencias sobre la entidad	Responder afirmativamente de UNA a CINCO preguntas
MAYOR	Genera altas consecuencias sobre la entidad.	Responder afirmativamente de SEIS a ONCE preguntas
CATASTRÓFICO	Genera consecuencias desastrosas para la entidad.	Responder afirmativamente de DOCE a DIECINUEVE

**Nota:** Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico.

Fuente: Departamento Administrativo de la Función Pública- DAFP (2022). Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 6.

### c. Criterios para el análisis de riesgos fiscales

- **Definición del nivel de probabilidad**

En la siguiente tabla se establecen los criterios para definir el nivel de probabilidad de los riesgos fiscales

Tabla 8. Criterios para definir la probabilidad de riesgos fiscales. UBPD, 2023

	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Departamento Administrativo de la Función Pública- DAFP (2022). Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 6

- **Calificación del impacto**

Para el caso de los riesgos fiscales, considerando la naturaleza y alcance de estos, y puesto que siempre tendrán un impacto económico, toda vez que el efecto dañoso ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública; para estos se aplicará la siguiente tabla:

Tabla 9. Criterios para definir el nivel de impacto de los riesgos fiscales. UBPD, 2023

	<b>AFECTACIÓN ECONÓMICA</b>
<b>Leve 20%</b>	Afectación menor a 10 SMLMV.
<b>Menor 40%</b>	Entre 10 y 50 SMLMV.
<b>Moderado 60%</b>	Entre 50 y 100 SMLMV.
<b>Mayor 80%</b>	Entre 100 y 500 SMLMV.
<b>Catastrófico 100%</b>	Mayor a 500 SMLMV.

Fuente: Departamento Administrativo de la Función Pública- DAFP (2022). Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 6

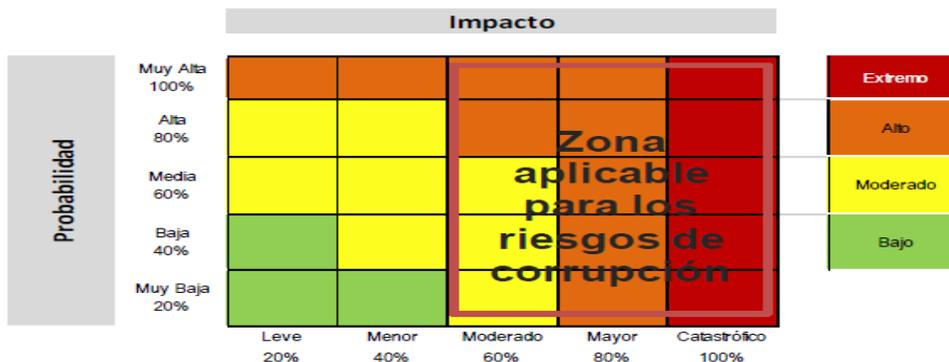
### 11.2.2 Evaluación de riesgos

La evaluación del riesgo es el producto de confrontar los resultados de la evaluación del riesgo inicial (riesgo inherente) frente a los controles establecidos, con el fin de determinar la zona de riesgo final (riesgo residual).

#### a. Determinación del nivel de severidad

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se determina la zona de riesgo inicial (RIESGO INHERENTE), o nivel de severidad donde se encuentra el riesgo. Para esto se utiliza el siguiente mapa de calor (Ilustración 1)

Ilustración 1. Mapa de calor para la determinación del nivel de severidad del riesgo inherente. UBPD, 2023



Fuente: Departamento Administrativo de la Función Pública- DAFP (2022). Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 6

Es importante señalar que, para el caso de los riesgos de corrupción, en la evaluación **NO APLICAN** los niveles de impacto insignificante y menor, ya que el análisis de impacto se realiza solo teniendo en cuenta los niveles “moderado”, “mayor” y “catastrófico”, debido a que estos riesgos siempre son significativos.

**b. Valoración de controles<sup>40</sup>**

Al momento de definir las actividades de control se debe validar que estas mitigan el riesgo, para lo cual se establece la siguiente estructura, tipología y atributos para los riesgos de gestión, fiscales y de seguridad de la información:



**Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificara el sistema que realiza la actividad.

**Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.

**Complemento:** corresponde a los detalles que permiten identificar claramente el objeto del control.

- **Atributos controles para riesgos de gestión y fiscales**

Acorde a lo anterior se presenta la siguiente tabla donde se muestran los atributos de eficiencia e informativos que deben tener los controles para la correcta mitigación de los riesgos de gestión y fiscales:

Características		Descripción	Peso	
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permite reducir el impacto de la materialización del riesgo, tiene un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sean manuales, procedimientos, flujogramas o	-

<sup>40</sup> El Control se define como la medida que permite reducir o mitigar el riesgo

Características		Descripción	Peso
			cualquier otro documento propio del proceso.
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva al riesgo.
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo.
	Evidencia	Con registro	El control deja un registro, permite evidenciar la ejecución del control.
		Sin registro	El control no deja registro de la ejecución del control.

Fuente: Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas – DAFP; Versión 6. Diciembre. 2022

Para los riesgos de seguridad de la información, los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo, quienes realizan la identificación y evaluación de controles existentes para cada una de las causas identificadas por cada uno de los riesgos. Esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas, para este caso se aplica la siguiente tabla:

CRITERIO DE EVALUACIÓN		TIPO DE CONTROL	PESO DEL CONTROL
¿Se considera un control Clave?		SI	10%
		NO	5%
Atributos de Eficiencia	Tipo	Preventivo	20%
		Detectivo	15%
		Correctivo	10%
	Implementación	Automático	20%
		Mixto	15%
		Manual	10%
Atributos informativos	Documentación	Documentado	10%
		Sin documentar	-
	Frecuencia	Continua	10%
		Aleatoria	-
	Registro	Con registro	10%
		Sin registro	-

**Nota:** Se podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2022 siempre y cuando se ajusten al análisis de riesgos. Estos controles se detallan en la "guía No 8 Controles de Seguridad y Privacidad de la Información" La cual se puede consultar en el siguiente enlace: [https://www.mintic.gov.co/gestion/i/615/articulos-5482\\_G8\\_Controles\\_Seguridad.pdf](https://www.mintic.gov.co/gestion/i/615/articulos-5482_G8_Controles_Seguridad.pdf).

A partir de los controles aplicados se puede disminuir el impacto o la probabilidad de ocurrencia de un riesgo, en la siguiente ilustración se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles. Los controles preventivos y detectivos disminuyen la probabilidad. Los controles correctivos disminuyen el impacto, cuando no se cuenta con este tipo de controles el impacto residual es el mismo calculado inicialmente.

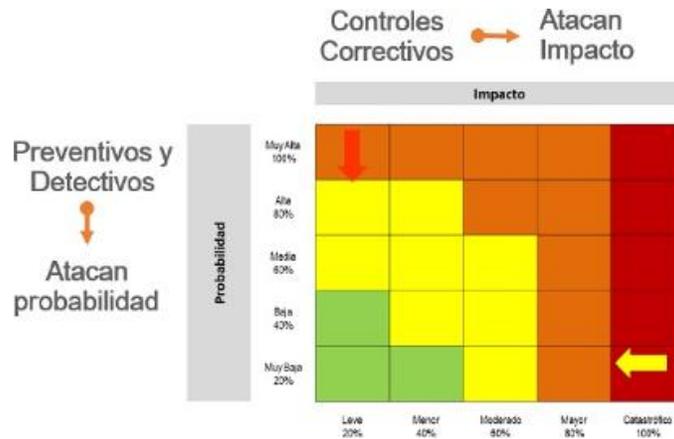


Ilustración 2. Movimiento en la matriz de calor acorde con el tipo de control. "Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP; Versión 6. Diciembre. 2022".

En el caso de los riesgos de corrupción al momento de definir las actividades de control se debe validar que estas mitigan el riesgo, para lo cual en su diseño se deben incluir las siguientes variables:

1. Definir el responsable de llevar a cabo la actividad de control.
2. Tener una periodicidad definida para su ejecución.
3. Indicar cuál es el propósito del control.
4. Establecer cómo se realiza la actividad de control.
5. Indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
6. Dejar evidencia de la ejecución del control.

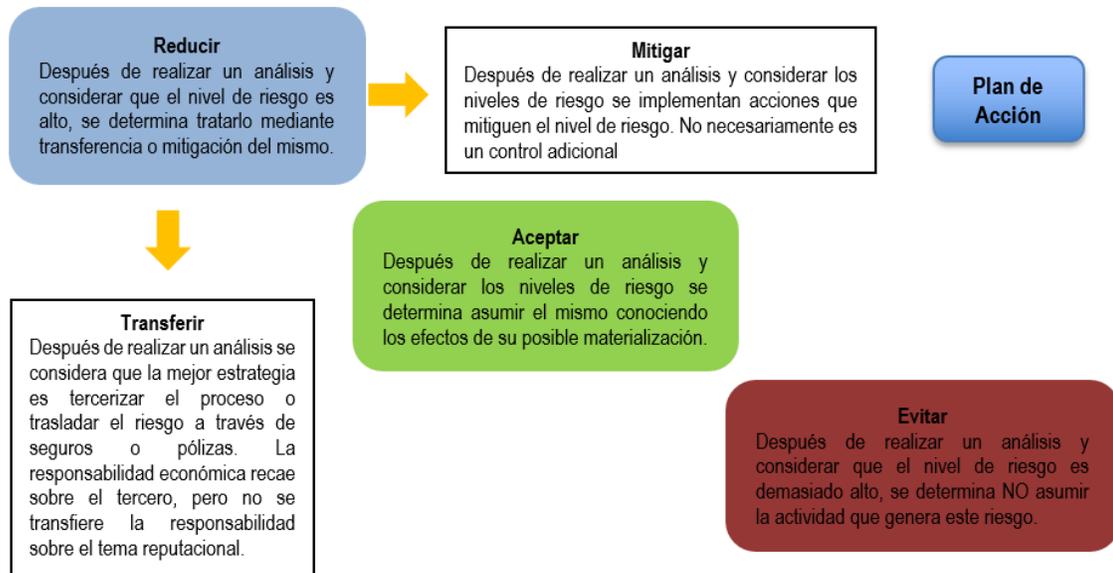
El líder del proceso, a partir de la metodología e instrumentos definidos, debe asegurar que las actividades de control se encuentran bien diseñadas y que éstas se ejecutan tal como han sido definidas, lo cual será revisado mediante las actividades de monitoreo de la segunda línea de defensa y, de auditoría interna o evaluación independiente realizadas por la Oficina de Control Interno (Tercera línea de defensa).

La forma en que estas actividades de control afectan la probabilidad y/o el impacto determina la ubicación final del riesgo en el mapa de calor (Ilustración 1), lo cual se conoce como riesgo residual.

## XII. ESTRATEGIAS PARA COMBATIR EL RIESGO

Luego de valorar el riesgo, el líder del proceso debe decidir si evita, reduce, comparte, transfiere o asume el riesgo, partiendo del riesgo residual de la siguiente manera:

- i) **Evitar el riesgo.** “Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo”<sup>41</sup>.
- ii) **Reducir el riesgo.** “Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo”<sup>42</sup>.
  - a) **Mitigar el riesgo:** “Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel del riesgo. No necesariamente es un control adicional”<sup>43</sup>.
  - b) **Transferir el riesgo:** “Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional”<sup>44</sup>.
- iii) **Aceptar el riesgo.** “Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización”<sup>45</sup>.



<sup>41</sup> Departamento Administrativo de la Función Pública, Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 5. 2020, pág. 57.

<sup>42</sup> *Ibíd.*

<sup>43</sup> *Ibíd.*

<sup>44</sup> *Ibíd.*

<sup>45</sup> *Ibíd.*

De esta manera se establecen los niveles de aceptación del riesgo para la UBPD (Apetito del riesgo):

- Riesgos ubicados en la **zona de riesgo baja** se asumirá el riesgo y los líderes de proceso realizarán seguimiento trimestral con el fin de validar que la calificación de probabilidad e impacto no ha tenido cambios. La administración de los riesgos en esta zona se realizará a través de las actividades propias del proceso.
- La UBPD no aceptará los riesgos ubicados en la zona de riesgo “moderado”, “alto” y “extremo”, por lo tanto, se adoptarán medidas para evitar, reducir o compartir el riesgo, de tal manera que se formularán planes de acción.
- Ningún riesgo de corrupción podrá ser aceptado, por lo tanto, para estos riesgos se adoptarán medidas para evitarlos, reducirlos o compartirlos, de tal manera que se formularán actividades de control sobre las cuales los líderes de proceso realizarán monitoreo y registro cuatrimestral, según lo definido en la Guía Estrategias para la construcción del plan anticorrupción y de atención al ciudadano.

El plan de acción como mínimo debe especificar: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento estos deben ser, “establecidos por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción”<sup>46</sup>.

### XIII. MONITOREO Y REVISIÓN DEL RIESGO

Es el paso que asegura el logro de los objetivos institucionales mediante la previsión de los eventos negativos asociados a la gestión de la entidad, y se desarrolla a través de un esquema de asignación de responsabilidades y roles de la siguiente manera:

Línea de defensa	Monitoreo y Revisión	Responsable
Línea estratégica	Definir el marco general para la gestión del riesgo y el control, y supervisar su cumplimiento.	Alta Dirección y el Comité Institucional de Coordinación de Control Interno.
1ª Línea de defensa	Desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.  Realizar monitoreo a las actividades de control formuladas realizando el registro y reporte de los avances a la Oficina Asesora de Planeación.	Líderes de procesos o líderes operativos de proyectos
2ª Línea de defensa	Asegurar que las actividades de control y los procesos de gestión de riesgos implementados por la primera línea de defensa estén diseñados apropiadamente y funcionen como se pretende.  Monitorear la gestión del riesgo y control ejecutada por la primera línea de defensa,	Oficina Asesora de Planeación, Oficina de Tecnología de Información y Comunicaciones, Secretaria General, coordinadores de equipos de trabajo, supervisores e interventores de contratos o proyectos, áreas financieras, comités de contratación (cuando aplique),

<sup>46</sup> Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, 2020.

	informando las observaciones pertinentes respecto a lo reportado con el fin de fortalecer el cumplimiento de las etapas de administración de riesgos y remitir a la (3ª línea de defensa), el resultado consolidado del monitoreo validado como segunda línea de defensa.	
3ª línea de defensa	<p>Proporcionar información sobre la efectividad del Sistema de Control Interno, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.</p> <p>Evaluar el diseño y ejecución de los controles con el fin de presentar un informe de evaluación a la gestión de riesgos ante la línea estratégica (Comité Institucional de Coordinación de Control Interno), tomando como insumo los resultados presentados por la 2ª línea de defensa, de acuerdo con lo definido en el plan anual de auditoría.</p>	Oficina de Control Interno

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas” Versión 5. Departamento Administrativo de la Función Pública. Año 2020

#### XIV. TRATAMIENTO DE RIESGOS MATERIALIZADOS

En el evento de materialización de un riesgo, las líneas de defensa deberán emprender acciones en el marco de sus responsabilidades, así:

Tratamiento de Riesgos Materializados	
1ª Línea de defensa	<ul style="list-style-type: none"> <li>• Informar y remitir a la segunda línea de defensa el respectivo plan de mejora que incluya <i>la ejecución de la corrección</i> que permitió restablecer la situación y las acciones a adelantar para la actualización del mapa de riesgos.</li> <li>• Cuando se trate de un riesgo de corrupción, realizar la denuncia ante la instancia de control correspondiente, una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normativa asociada al hecho de corrupción materializado).</li> </ul>
2ª Línea de defensa	<ul style="list-style-type: none"> <li>• Orientar a los líderes de proceso en la actualización del mapa de riesgos.</li> </ul>
3ª Línea de defensa	<ul style="list-style-type: none"> <li>• Cuando en el marco de un ejercicio de evaluación independiente o seguimiento, la Oficina de Control Interno identifique la materialización de un riesgo, deberá informar a los líderes de proceso sobre el hecho detectado, los cuales emprenderán las acciones descritas para la primera línea de defensa en este numeral.</li> <li>• Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso para revisar el mapa de riesgos.</li> <li>• En articulación con la segunda línea de defensa, informar a la línea estratégica (Comité Institucional de Coordinación de Control Interno) sobre el estado de los riesgos materializados.</li> </ul>

Para los riesgos de corrupción, en el caso de que se tenga la presunta materialización de un riesgo, es necesario informar lo antes posible a la entidad, para lo cual se han habilitado tanto el correo [soytransparente@ubpdbusquedadesaparecidos.co](mailto:soytransparente@ubpdbusquedadesaparecidos.co), canal de denuncia contra “presuntos” hechos que atenten

contra la transparencia en la gestión, como la opción de denuncia en el formulario de PQRSD, ubicado en el portal web de la UBPD, para que ciudadanas y ciudadanos puedan realizar oportunamente la denuncia ya sea identificándose o de manera anónima. Es importante que cuando se realicen este tipo de denuncias se adjunten todas las pruebas posibles que las justifiquen y/o evidencien.

El aplicativo dirige esta denuncia automáticamente al soporte jurídico del Grupo Interno de Trabajo de Servicio al Ciudadano, quien manualmente completa la información requerida, clasifica el tipo de solicitud y asigna a la dependencia correspondiente.

La denuncia se asigna a la Secretaría General, como responsable del proceso de Control Interno Disciplinario en la UBPD, para garantizar un doble control. Siempre se copia a la Oficina Asesora Jurídica, dependencia que asumirá el proceso de investigación. En el caso de que la acusación de un presunto acto de corrupción recaiga sobre integrantes de la Secretaría General, se debe contestar en los términos establecidos en la solicitud, dando la mayor prioridad a estas posibles materializaciones.

De manera paralela a la asignación, siempre se copia a la Oficina Asesora de Planeación, mediante correo electrónico, con la siguiente información básica de la denuncia de corrupción, para garantizar la confidencialidad de la información: 1) fecha de la solicitud, 2) dependencia asignada al proceso de investigación, 3) plazo oportuno de respuesta, para que se pueda hacer el monitoreo oportuno con las siguientes acciones:

- Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles
- Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción
- Llevar a cabo un monitoreo permanente

Si como resultado del proceso de investigación interna de la entidad, se verifica la materialización de un presunto hecho de corrupción, se debe comunicar inmediatamente a las autoridades competentes.

## **XV. EVALUACIÓN**

La evaluación de la política de administración de riesgos se realizará cada vez que se requiera por parte de la alta dirección.

## **XVI. MONITOREO Y REVISIÓN**

El monitoreo y revisión al mapa de riesgos institucional, estará a cargo de los líderes de los procesos, en conjunto con su equipo de trabajo (primera línea de defensa) y de los líderes de cada uno de los tipos de riesgos en la Entidad (segunda línea de defensa), su finalidad principal es monitorear permanentemente la gestión del riesgo y la efectividad de los controles, y de esta manera, sugerir los correctivos y ajustes cuando sea necesario para asegurar un efectivo manejo de riesgo.

El monitoreo al mapa de riesgos de gestión y de seguridad de la información, así como a los controles establecidos, se realizará como mínimo (1) vez al año, salvo en los casos que los lineamientos u orientaciones establezcan los respectivos seguimientos. Los ciclos de control establecidos se revisarán y ajustarán si es necesario, para adaptarlos a los cambios, situaciones o circunstancias por las que pueda atravesar la Entidad.

Para el caso de los riesgos de corrupción el monitoreo se realizará cuatrimestralmente desde el inicio de cada vigencia.

## **XVII. SEGUIMIENTO Y EVALUACIÓN INDEPENDIENTE**

La Oficina de Control Interno en su rol de evaluación de la gestión del riesgo, realizará el seguimiento al mapa de riesgos institucional, atendiendo la normatividad aplicable.

## **XVIII. DIVULGACIÓN**

La Política de Administración del Riesgo y el Mapa de Riesgos Institucional se divulgarán en la Entidad, a través de los canales y medios de comunicación establecidos por el líder de la administración del riesgo en la Entidad. La socialización al interior de las dependencias estará a cargo de los líderes de proceso.

Para el caso del mapa de riesgos de corrupción, este será publicado en la página web de la entidad, a más tardar el 31 de enero de cada vigencia.

Revisó: Miembros del Comité Institucional de Control Interno en la sesión 1 del día 29 de enero de 2024  
Aprobó: Miembros del Comité Institucional de Control Interno en la sesión 1 del día 29 de enero de 2024